AO 106 (mod. 5/14) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

One Samsung Galaxy Model SM-G955U cellular phone, IMEI 357751080604686

Case No. 17-M-713

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property: See attached affidavit and attachments hereby incorporated by reference.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:
Evidence of a violation of Title 18 U.S.C. Sections 2251, 2252, and 2252A as set forth in affidavit and attachments.

The application is based on these facts: See attached affidavit.

Nathan A. Cravatta
Applicant's signature

Nathan A. Cravatta, Special Agent
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 11/9/17

Judge's signature

City and State: Green Bay, Wisconsin

James R. Sickel, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Nathan A. Cravatta, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of criminal complaints and search warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as a Special Agent with HSI since May 2005. I am currently assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin.

3. My experience as an HSI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of federal law involving child exploitation, including the production, transportation, receipt,

distribution and possession of child pornography. I have received training and have gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications and the execution of searches and seizures involving computer crimes. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children which constituted violations of Title 18, United States Code, Sections 2251, 2252 and 2252A.

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, incorporated herein by reference as if fully set forth, are located in the Device for which authority is requested to search. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property (here after known as the "Device") to be searched is:

a. Samsung Galaxy Model SM-G955U cellular phone, IMEI 357751080604686

6. The Device is currently located at the U.S. Department of Homeland Security-Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, #600, Milwaukee, Wisconsin 53202.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

8. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography).

APPLICATION A

9. "Application A" is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos.

10. Once downloaded and installed, the user also has a display name, which will be what other users initially see when transmitting messages back and forth. As part of the account creation process, "Application A" users are asked to supply a valid e-mail address, create a password, provide an optional date of birth, and user location. The user also has the option of uploading a "profile avatar" that is seen by others. Once

the "Application A" user has created an account, the user is able to locate other users via a search feature. The search feature usually requires the user to know the intended recipient's username. Once another user is located or identified, Kik users can send messages, images, and videos between two parties.

11. "Application A" also allows users to create chat rooms, of up to 50 people, to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created "Application A" users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword.

12. "Application A" users frequently advertise their "Application A" usernames on various social networking sites in order to meet and connect with other users. In some cases, "Application A" also provides various avenues, such as dating sites and social media applications, for meeting other users. HSI undercover agents observed in some chats that many of the users stated they felt safe using "Application A" as a means of trading child pornography and for other illegal activities, due to the fact that ""Application A" is a Canadian based company, and not subject to the same United States laws." HSI undercover agents have noted messages posted in "Application A" chat rooms relating to the enforcement, deletion, or banning of users and rooms by "Application A" for the purpose of exchanging or distributing child

pornography. HSI agents noted the comments to include the continued creation of new rooms and new user accounts to circumvent "Application A"s enforcement efforts.

PEER TO PEER PROGRAMS

13. Based on my training and experience, I know that a frequently employed method to share data over the Internet is Peer-to-Peer (P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of widely available software. The software is designed to allow users to trade digital files through the Internet. There are several different software applications that can be used to access these P2P networks and these applications operate in essentially the same manner.

14. To access the P2P networks, a user first obtains the P2P software, which can be downloaded free from the Internet. This software is used for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available for download by any other user connected to the P2P network.

15. A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search. The results supplied from that keyword search are

displayed and the user then selects file(s) which he/she wants to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Oftentimes, a forensic examiner, using these logs, can determine the IP address from which a particular file was obtained.

16. Most P2P software does not display the IP address of the person sharing the file to the user. Third party software is available to identify the IP address of the P2P computer sharing a particular file.

17. The Gnutella2 network is a very popular and publically available P2P file-sharing network. Most computers that are part of this network are referred to as "peers" or "clients." A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients. The Gnutella2 network can be accessed by peer/client computers via many different Gnutella2 network client (software) programs, including uTorrent, Vuze, and others. These are publically available and typically free P2P client software programs that can be downloaded from the Internet. Gnutella2 sets up its searches by keywords typically on torrent websites. The results of a keyword search are displayed to the user. The website does not contain the files being shared, only the file referred to as a "torrent." A torrent file defines the files being shared and contains file names, file sizes, file path(s), the total number of pieces, the size

of each piece, the SHA-1 hash value of each piece, and the torrent type (public or private). The torrent file does not contain the desired content; it simply defines what is available. A user may then select a torrent file(s) from the search results for download. For example, a person interested in obtaining child pornography images/videos could open the Gnutella2 website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user selects a torrent from the results displayed the file(s) he/she wants to download. Once the torrent file is downloaded, it is used by a Gnutella2 program, which the user had previously installed. The file(s) is downloaded directly from the computer or computers sharing the file. The users can receive pieces of the selected file from numerous sources at once. Once received, the pieces are then reassembled into the entire selected file. The downloaded file(s) is stored in a folder previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file will remain until moved or deleted. Multiple files may be downloaded in parallel. This means that the user can download more than one file at a time.

18. An "info hash" is used to uniquely identify a torrent. For example, when a client establishes communication with a peer, it identifies the torrent that it is interested in by providing the info hash. The info hash assures that all the values in the info section of the torrent that is sought is identical to the values of the info section in the target's torrent.

SUMMARY OF INVESTIGATION INVOLVING "APPLICATION A"

19. Canadian law enforcement officers have reported to HSI that on March 22, 2016, an officer with the Saskatchewan Police Service (SPS) in Saskatchewan, Canada, arrested an individual (hereinafter "John Doe") for parole violations.[1] Pursuant to the arrest, SPS seized John Doe's iPhone. John Doe told SPS that he had been using an online mobile chat application to download and distribute child pornography images and videos to a network of other users of the mobile chat application. He provided SPS his username and login information for the "Application A" and gave SPS consent to take over and use his account to conduct investigations and gather evidence. This chat application is hereinafter referred to as ""Application A"."[2] HSI was not involved with the user's arrest.

20. SPS was able to log in and secure John Doe's "Application A" account. In reviewing the chat conversations held with John Doe's account, SPS was able to identify 72 unique "Application A" users who had shared at least one image or video of child pornography with John Doe directly, or who had posted child pornography in one of the "Application A" groups to which John Doe belonged, and six "Application A" users

---

[1] John Doe's true name is known to law enforcement. This investigation remains active and disclosure of Doe's true name would potentially alert investigative suspects to the fact that law enforcement action is being taken, thereby provoking suspects to notify other users of law enforcement action, flee, and/or destroy evidence.

[2] The actual name of "Application A" is known to law enforcement. This chat application remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as "Application A."

who had posted a message between or commented on child pornography images or videos. Many of the groups to which John Doe belonged had names that included terms that your affiant knows through training and experience to be suggestive of child pornography.

21. SPS logged all of the information regarding the messages and saved all of the images and videos of child pornography shared with John Doe's account. SPS sent preservation requests to "Application A" regarding all 78 accounts referenced in the previous paragraph between April 20 and April 30, 2016. SPS transmitted to HSI the information logged and saved from the review of John Doe's "Application A" account.

22. On June 28, 2016, a Production Order was issued by a Provincial Court Judge in Saskatchewan, Canada, ordering "Application A" to produce user information and saved content regarding these 78 accounts. On September 15, 2016, SPS received the requested results from "Application A". The information received from "Application A", including the Certification of Records provided by "Application A", was transmitted to HSI, along with a copy of the Production Order issued by the Provincial Court Judge.

23. The results provided by "Application A" included, among other things, additional images and videos of child pornography recently shared by the 78 accounts. This included both child pornography shared with John Doe and child pornography shared with other individuals and groups not related to John Doe's account. Additional Production Orders were served on "Application A" for information regarding the

"Application A" accounts who shared child pornography with the originally investigated 78 accounts, leading to the identification of additional "Application A" accounts beyond the 78 accounts that shared child pornography with John Doe.

24. Your affiant has reviewed the information received from "Application A". A review of that information shows that on October 25, 2015 an "Application A" user with the account name "brewcrewbassman" used "Application A" to share images of child pornography. Specifically, the images shared by "brewcrewbassman" included the following:

a. A still color image of a juvenile female approximately three to four years old who is lying on her back with her legs being spread by an adult female who is holding the girl's ankles. The girl is wearing a multi-colored horizontal striped shirt with no bottoms. Her unclothed vagina and buttock are visible in the image. The adult female is positioned behind the juvenile female and is wearing a gray long sleeved shirt with pink lettering and blue jeans. The word "Bad" is visible on the front of the adult female's shirt. This image was shared with a group of other Application users on October 25, 2015 at 19:29:33 Coordinated Universal Time (UTC).

b. A still color image of a juvenile female approximately three to four years old who is lying on her back with her legs being spread by an adult female who is holding the girl's ankles. The girl is wearing a

multi-colored horizontal striped shirt with no bottoms. Her unclothed vagina and buttock are visible in the image. The adult female is positioned behind the juvenile female and is wearing a gray long sleeved shirt with pink lettering and blue jeans. The word "Bad" is visible on the front of the adult female's shirt. This image was shared with a group of other Application users on October 25, 2015 at 19:29:42 UTC.

c. A still color image of juvenile female who is approximately six to seven years old who is sitting on a bed with a light blue and blue checkered blanket. A white and green colored wall is visible in the background. She is wearing blue jeans and a pink and yellow tank top. She is holding an infant on her lap who is wearing a pink long sleeved shirt. Her hands are grasped around the back thigh area of the infant and the infant's legs are raised exposing the vaginal and buttock area. This image was shared with a group of other Application users on October 25, 2015 at 20:10:13 UTC.

d. A still color image of juvenile female who is approximately six to seven years old who is sitting on a bed with a light blue and blue checkered blanket. A white and green colored wall is visible in the background. She is wearing blue jeans and a pink and yellow tank top. She is holding an infant on her lap who is wearing a pink long sleeved shirt.

Her hands are grasped around the back thigh area of the infant and the infant's legs are raised exposing the vaginal and buttock area. This image was shared with a group of other Application users on October 25, 2015 at 20:10:13 UTC.

25. Your affiant has reviewed additional information received from "Application A". A review of that information shows that on March 22, 2016 an "Application A" user with the account name "brewcrewbassman" used "Application A" to share an image of child pornography. Specifically, the image shared by "brewcrewbassman" included the following:

a. A still image of a female approximately two to three years of age who is leaning over at the waist with her legs spread. Her hands are positioned in front of her on what appears to be a wooden floor. Her face is partially visible in the image and is obstructed by her clothing. She is wearing a pink skirt or shirt which is positioned above her waist exposing her buttock and vaginal area. This image was shared with a group of other Application users on March 22, 2016 at 17:02:24 (UTC). It should be noted "brewcrewbassman" shared an additional image to the same group of Application users on March 31, 2016 at 04:24:23 UTC, but this image appears to be child erotica.

26. The information provided by "Application A" included IP addresses used by the target account. Specifically, IP address 162.195.41.180 was used by

"brewcrewbassman" on October 25, 2015, March 22, 2016. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 162.195.41.180 was registered to AT&T Internet Services.

27. On July 20, 2017, a Department of Homeland Security summons was issued to "Application A" requesting updated subscriber and usage information for "Application A" user "brewcrewbassman." Information subsequently provided indicated "brewcrewbassman" was noted as being in "America/Chicago" with a reported IP address of 162.195.41.180 on May 7, 2017 at 02:12:17 UTC. "Application A" provided information indicating the account for "brewcrewbassman" was registered on May 4, 2015. An email address of brewcrewbassman@gmail.com was provided by the registered user.

28. On July 24, 2017, a Department of Homeland Security summons was issued to AT&T, Inc., Global Legal Demand Center, requesting subscriber information related to IP address 162.195.41.180 being used on the above mentioned date and time. A review of the results obtained on August 3, 2017 identified the following account holder and address: Thomas Daul, 1818 South Adams Street, Appleton, Wisconsin 54915-1343.

SUMMARY OF INVESTIGATION INVOLVING GNUTELLA 2 NETWORK

29. On January 5, 2017, a Wisconsin Department of Justice, Division of Criminal Investigation (DCI) special agent, acting in an undercover capacity (UC-1),

attempted to obtain a list of files being shared on the Gnutella 2 network by a device utilizing IP address 162.195.41.180. This IP address reported eleven files being shared on the Gnutella 2 network, of which two files were of investigative interest and possibly contained child pornography images based on a list of known info hashes. UC-1 directly connected to a device at IP address 162.195.41.180. The device reported it was using client software Shareaza 2.7.9.0.

30. On Thursday, January 5, 2017, between 2314 and 2317 hours, UC-1 successfully downloaded two files that a device at IP address 162.195.41.180 was making available. The device at IP Address 162.195.41.180 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

31. UC-1 reviewed the downloaded files, and determined the files were child pornography.

32. On January 5, 2017, UC-1 queried the IP address 162.195.41.180 through the American Registry for Internet Numbers (ARIN). ARIN reported IP address 162.195.41.180 registered to AT&T Internet Services.

33. After reviewing the files downloaded by UC-1, the files are described as follows:

a. File name: "pictures from ranchi torpedo dloaded in 2009-pedo kv kidzilla pthc toddlers 0yo 1yo 3yo 4yo 5yo 6yo 9yo tara babyj(135).jpg". This is a still color image of a prepubescent girl who is wearing pink tank top shirt, kneeling to the right of a nude

pubescent teenage male. The male in lying on his back, with his underwear pulled down to his knee. He is looking up towards the camera which is positioned near his feet and legs. The prepubescent girl is seen performing fellatio upon the teenage boy's unclothed and erect penis. The boy's unclothed penis and scrotum are both clearly visible and are the focal points of this image.

b. File name: "pictures from ranchi torpedo dloaded in 2009-pedo kv kidzilla pthc toddlers 0yo 1yo 3yo 4yo 5yo 6yo 9yo tara babyj(139.jpg" This is a still color image of a nude prepubescent girl who is seated upon a bed, facing towards the camera. The girl's legs are spread widely and the fingers of her left hand are touching her unclothed vaginal area. The girl's unclothed and undeveloped breasts, along with her unclothed vaginal area, are both clearly visible and are the focal points of the image.

34. On August 29, 2017, a Department of Homeland Security summons was issued to AT&T, Inc., Global Legal Demand Center, requesting information related to IP address 162.195.41.180 being accessed on January 5, 2017 at 2314 hours. A review of the results obtained on August 30, 2017 identified the following account holder and address: Thomas Daul, 1818 South Adams Street, Appleton, Wisconsin 54915-1343.

35. A check of publicly available databases revealed that Brandon Daul and Thomas Daul reside at 1818 South Adams Street, Appleton, Wisconsin 54915-1343.

PAST CHILD EXPLOITATION CONDUCT OF BRANDON DAUL

36. According to reports received from the Appleton Police Department, on May 14, 2011, an individual residing in Manitowoc, Wisconsin was chatting on an online chatting service known as Yahoo! Chat with a subject using the user name "metal_brand." During the course of this conversation, "metal_brand" indicated he had just performed oral sex on his three year old niece. "Metal_brand" also indicated he had performed other sexual acts on this minor female. "Metal_brand" was later identified as being Brandon T Daul. A computer seized during a search warrant conducted at the residence of Brandon Daul resulted in the discovery of approximately 80 images and 27 videos depicting child pornography on a computer. Daul was subsequently arrested for Possession of Child Pornography (5 counts). He was later sentenced in Outagamie County Circuit Court to three years in prison for each count to be served concurrently followed by five years of extended supervision. He was released from prison on October 7, 2014 and is currently on extended supervision.

EXECUTION OF A SEARCH WARRANT AND SUBSEQUENT INTERVIEW OF BRANDON DAUL

37. On October 25, 2017, officers and agents with HSI, DCI, and Appleton Police Department executed a search warrant at 1818 South Adams Street, Appleton, Wisconsin. Brandon Daul was not located at the residence during the execution of the search warrant. A subsequent search of the residence resulted in the seizure of a laptop

computer, numerous cellular telephones, a Play Station 4 gaming system, and several miscellaneous documents. The laptop computer was discovered in the bedroom of Brandon Daul. An initial forensic review of the laptop computer and Samsung cellular telephone did not result in the discovery of any images or files depicting child pornography. A complete forensic examination on all electronic devices is ongoing.

38. On this date, Brandon Daul was located at his place of employment located in Menasha, Wisconsin and consented to being interviewed by law enforcement. Daul indicated he did own a cellular telephone and had the Device in his possession. He explained it was condition of his extended supervision that he not possession any electronic device. He acknowledged he has owned the Device since approximately April 2017. He also indicated he previously owned and used a Samsung Galaxy S5 cellular telephone and has this device for approximately two years. Daul stated he was familiar with "Application A" and he did use this application on his Samsung Galaxy S5 in approximately 2015. Daul indicated while using this application, his user name was "brewcrewbassman" and he registered the account with email address brewcrewbassman@gmail.com. He acknowledged he did frequent various "chat" groups while using the application. When questioned further, Daul indicated he wished to have an attorney present before answering additional questions. Daul was placed into custody by the Appleton Police Department for a violation of his extended supervision and the Device was turned over to and detained by HSI.

TECHNICAL TERMS

39. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks

c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their

recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

d. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless

communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

40. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at https://www.samsung.com/us/mobile/phones/galaxy-s/galaxy-s8-plus-64gb--verizon--midnight-black-sm-g955uzkavzw/, I know that the Samsung Galaxy Model SM-G955U cellular telephone has capabilities that allow it to serve all or some of the following functions: wireless telephone, a digital camera, portable media player, GPS

navigation device, PDA, and accessing /downloading information from the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

41. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

42. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

43. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

44. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

45. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Nathan A. Cravatta
Special Agent
U.S. Department of
Homeland Security

Sworn and subscribed before me this 9th day of November, 2017.

James R. Sickel
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a:

a. Samsung Galaxy Model SM-G955U cellular phone, IMEI 357751080604686

The Device is currently located at the U.S. Department of Homeland Security-Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, #600, Milwaukee, Wisconsin 53202.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 USC 2251, 2252 and 2252A, including:

   a. Records containing child pornography or pertaining to the production, distribution, receipt, or possession of child pornography;

   b. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors;

2. All names, aliases, and numbers stored in the Device, including numbers associated with the Device, relating to the identities of those engaged in the production, possession, receipt, or distribution of child pornography.

3. Images or visual depictions of child pornography.

4. Records and information containing child erotica, including texts, images and visual depictions of child erotica.

5. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the violations.

6. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing the violations.

7. The list of all telephone calls made or received located in the memory of the Device that provides information regarding the identities of and the methods and means of operation and communication by those engaged in the possession, receipt, or distribution of child pornography.

8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography

9. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

10. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.